Declaration
of
Dr. Andrew Stivers

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

DECLARATION
OF
DR. ANDREW STIVERS

JULY 12, 2024

BERNADINE GRIFFITH, et al.,

individually and on behalf of all

others similarly situated,

Plaintiffs,

v.

TIKTOK, INC., a corporation,

BYTEDANCE, INC., a corporation,

Defendants

Case No. 5:23-cv-00964-SB-E
United States District Court for the Central District of California

Table of Contents

I. Work Performed

A. Qualifications

1. I am an economist and Managing Director at NERA Economic Consulting. NERA is a global firm of experts dedicated to applying economic, finance, and quantitative principles to complex business and legal issues. I received my Ph.D. in economics from the University of Texas. Prior to joining NERA in 2021, I was the Deputy Director for Consumer Protection in the Bureau of Economics at the Federal Trade Commission. In this role I oversaw all internal economic analysis on consumer protection matters at the Commission and advised the Commissioners and Bureau of Consumer Protection leadership on the economics of privacy and consumer protection cases.

2. My area of expertise is in the economics of consumer protection, including privacy, which is based on my knowledge, training, and research in the economics of consumer markets and experience evaluating deceptive and unfair practices at the FTC. I have experience analyzing firm privacy, marketing and pricing practices, consumer responses to those practices and in calculating damages in connection with alleged consumer protection violations. As the lead economist for consumer protection work at the FTC, I advised the Commission on issues related to consumer confusion, deception, fraud, unfairness, damages, ill-gotten gains, and penalties. My research has appeared in *Journal of Consumer Policy, Information Economics and Policy* and *Managerial and Decision Economics*. My publications are listed in my curriculum vitae, which is appended to this report as Appendix I.

B. Background on the Matter

3. TikTok Inc. ("TTI") provides the TikTok platform ("TikTok") in the United States that allows users to create, view and share videos online. TTI also provides products to other businesses as part of its "TikTok for Business" line. This line includes the TikTok Pixel and Events API. These products are tools that can be configured by website operators to transmit certain types of information related to how users of websites interact with those sites. Certain information is shared with TTI that can in some cases allow TTI to connect it with its users. This kind of information transmission is common across online platforms and used online for a variety of marketing and analytic purposes.

C. Understanding of Plaintiffs' Allegations

4. I understand that Plaintiffs Griffith, Shih and Watters allege that they are not TikTok users and that they allege that data related to them was collected, stored, and used by TTI. Plaintiffs allege that TTI's practices cause a variety of privacy violations and related claims. They allege that they have suffered economic injury caused by those alleged violations that meet the requirements for certification as a class.

5. I understand that the Plaintiffs are seeking to certify a number of classes and subclasses. I understand that each class or subclass is based on non-TikTok users whose data is alleged to have been transmitted to TTI from websites that use the TikTok Pixel between March 2022 and the present. The Plaintiffs propose classes or subclasses that vary by geography (all of the United States or limited to California), whether the Events API was also used, whether non-TikTok users allegedly blocked third-party cookies, and how Pixel was allegedly configured. Alternatively, the Plaintiffs seek to certify classes or subclasses by website and by geography.

D. Assignment

6. Counsel for Defendants have asked me to offer opinions, from an economic perspective, on consumer understanding, preferences and behavior with respect to their online privacy practices relevant to Case No. 5:23-cv-00964-SB-E pending in the United States District Court for the Central District of California. Specifically, I have been asked to analyze:

   a. Whether internet users are aware that their data is transmitted, stored, processed and used when they use the internet;

   b. Whether the value or cost to internet users of such data practices can be assessed using a unified framework;

   c. Whether 'consumers' online behaviors with respect to privacy concerns and privacy disclosures are homogenous; and,

   d. How those issues apply to the class(es) proposed by the Plaintiffs in this case.

7. NERA is compensated for the time that I spend in connection with this matter at my standard hourly rate of $750 and is separately reimbursed for reasonable out-of-pocket

expenses. NERA is also compensated for the time spent by staff assisting me on this assignment at their standard hourly rates. Neither my compensation nor NERA's is dependent on the outcome of this litigation.

E. Materials Relied Upon

8. My review of the testimony and documents, as well as my independent research spans a wide variety of parties and sources, including those of the Defendants and various publicly available sources. In addition, I have relied on my experience and training as an applied microeconomist. A complete list of the information that I considered in preparing this report can be found appended to this report as Appendix II. The specific information upon which I have relied is cited in the footnotes of the text. My work in this matter is ongoing. Accordingly, I reserve the right to supplement these opinions based on, for example, the receipt or analysis of additional relevant information or data, or if additional research, reflection, or the correction of inadvertent errors leads me to change my opinions.

F. Summary of Preliminary Conclusions

9. Based on my analysis to date, I have reached the following preliminary conclusions:

a. Consumers using the internet understand that their data is transmitted, stored, processed, and used in some cases to provide them personalized ads in exchange for services and content.
b. Potential consumer privacy harm varies widely depending on the context and their specific preferences and cannot be presumed from either a common mechanism or from common behaviors.
c. Privacy policies vary widely across websites, and consumers vary widely in terms of their use and interpretation of those privacy policies.
d. Consumers have a wide variety of behaviors and tools they use to manage their online privacy.
e. The complaint shows that the named Plaintiffs' alleged privacy harms are idiosyncratic and context dependent.

II. Framework for the Analysis

10. I understand from the Second Amended Complaint and the Plaintiffs' Memorandum in Support of Their Motion for Class Certification that they are alleging that the purported class could encompass almost any internet user who also was not a TikTok user. This means that purported Class Members would match the characteristics and understanding of the general American adult population. I present evidence on how this population understands privacy online, and the actions individuals take based on those understandings, which cannot be homogenously understood or categorized. I also present evidence on the bases for any privacy harms, or lack thereof, for this population, and the widely varied preferences and contexts that would underlie any such harms. Finally, I present evidence on how American adults interact with privacy disclosures on the websites that they visit.

11. With this analysis on how Americans understand and behave with respect to online privacy I turn to how the descriptions of the named Plaintiffs' alleged privacy harms in the Second Amended Complaint illustrate the same varied bases and contexts for those alleged harms.

III. Expert Opinions

A. Consumers Using the Internet Understand That Their Data is Collected, Stored, Processed and Used in Some Cases to Provide Them Personalized Ads in Exchange for Services and Content

12. Americans are aware that companies collect and use data about them and their online activity. In a 2019 study, 91 percent of all American adults said that they understand at least some of their online activity is tracked by companies.[1] Similarly, 77 percent were aware specifically of targeted advertising, and 64 percent reported specifically seeing ads or promotions that they believed to be personalized for them.[2]

13. Regardless of specific knowledge of targeted advertising, Americans broadly understand that their online activity is not private. A prominent review of economic

[1] Brooke Auxier *et al*, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 2019) at 25 (available at https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf) (hereafter *Auxier (2019)*).

[2] *Id.* at 7.

research on privacy from 2016 found that "surveys of US respondents have repeatedly highlighted privacy as one of the most significant concerns of Internet users…"[3] and this finding has not changed in more recent surveys. For example, the Pew Research Center reported in 2023 that 81 percent of American adults "are concerned with how companies use the data they collect about them."[4]

14. Furthermore, most Americans say that they do not understand, or have control of, how data related to their behavior are collected or used. For example, 78 percent of Americans believe that they are making the right privacy decisions, but the majority of these (61 percent) believe that those decisions may not have much effect.[5] 67 percent of Americans say they do not believe that they understand how that data is used.[6] Overall, 73 percent of Americans do not believe that they have control over what companies do with their data.[7]

15. However, even in the face of these well-known concerns, internet use is ubiquitous in America. In 2023, 95 percent of American adults' report being users of the internet.[8] 85 percent of American adults reported being online at least daily.[9] People use the internet for a wide range of activities, from entertainment to shopping, and for work.[10]

16. Privacy scholars and advocates have spent considerable time arguing over whether there is a "privacy paradox," where there is a supposed disconnect between people's stated preference for privacy and their general failure to act as though privacy was as

[3] Alessandro Acquisti *et al*, "The Economics of Privacy," *Journal of Economic Literature* 54(2) (2016) 442-492 at 449 (available at *http://doi.org/10.1257/jel.54.2.442*) (hereafter *Economics of Privacy*).

[4] Colleen McClain *et al*, *Views of Data Privacy Risks, Personal Data and Digital Privacy Laws*, Pew Research Center (October 2023) (available at https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/).

[5] *Ibid.*

[6] *Ibid.*

[7] *Ibid.*

[8] "Internet and Broadband Fact Sheet," *Pew Research Center* (January 2024) (available at https://www.pewresearch.org/internet/fact-sheet/internet-broadband/) (accessed 6/17/2024).

[9] Andrew Perrin and Sara Atske, "About three-in-ten U.S. Adults say they are 'Almost Constantly' Online," *Pew Research Center* (March 2021) (available at https://www.pewresearch.org/short-reads/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/).

[10] NTIA, "Most popular online activities of adult internet users in the United States as of November 2021," *Statista* (available at https://www.statista.com/statistics/183910/internet-activities-of-us-users/) (accessed at 6/27/24).

concerning as they say.[11] However, more generally, researchers on consumer attitudes and behaviors have long recognized that stated attitudes do not necessarily predict how consumers make real-world decisions.[12]

17. For example, a variety of surveys have found that consumers say that they are willing to pay substantially more for "ethically produced" products like Fair Trade coffee.[13] When purchasing behavior was actually tested, an experiment at a high-end grocery store chain found that "[w]hile consumers attach value to ethical sourcing, there is significant heterogeneity in willingness to pay for it." In other words, not everyone who said that they would pay for it did. In discussion of the results, the authors note that both idiosyncratic attributes and store context could drive that result.[14]

18. Conversely, people may clearly see a potential cost to an activity, but believe that the benefit is greater, and so still do that activity. For example, they might acknowledge that eating a bowl of ice cream is unhealthy while still eating the ice cream anyway.

19. In the same way, people can believe that there is a privacy cost in being online, and still decide that they are getting a net benefit from their online activity. That benefit can be substantial. For example, a recent study of the value of "digital goods" found significant value to consumers associated with using a variety of popular, free online services.[15] The authors estimated that the median consumer in 2017 valued search engine services at $17,530 per year, email at $8,414 per year, and digital maps at $3,648 per year. Content was also valuable, with video, social media, and music worth $1,663 to the

[11] See *e.g.* Daniel J Solove, "The Myth of the Privacy Paradox," *George Washington Law Review* 89 (2021) 1-51 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265); *see also* Susan Athey *et al.,* "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," *National Bureau of Economic Research* (2017) (available at https://www.nber.org/papers/w23488).

[12] Icek Ajzen *et al*, "The Influence of Attitudes on Behavior," in Dolores Albarracin *et al* eds., *The Handbook of Attitudes Volume 1: Basic Principles* (New York, NY: Routledge, 2019) (available at https://people.umass.edu/aizen/pubs/aonb.pdf).

[13] See *e.g.* Patrick Pelsmacker *et al*, "Do Consumers Care about Ethics? Willingness to Pay for Fair-Trade Coffee," *Journal of Consumer Affairs* 39(2) (2005) at 361–383 (available at https://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2005.00019.x).

[14] Jens Hainmueller *et al*, "Consumer Demand for Fair Trade: Evidence from a Multistore Field Experiment," *Review of Economics and Statistics* 97(2) (2015) 242-256 (available at https://web.stanford.edu/~jhain/Paper/REST2015.pdf).

[15] Erik Brynjolfsson *et al*, "The Digital Welfare of Nations: New Measures of Welfare Gains and Inequality," *National Bureau of Economic Research* (2023) at 3-4 (available at https://www.nber.org/papers/w31670).

median consumer. Adding in e-commerce ($842) and messaging ($155) brings the total value to $32,252, a 26 percent increase from 2016.[16]

20. Researchers have also found that the quality and availability of online content is dependent on the premium associated with personalized content.[17] The overall benefits of personalized ads in providing otherwise free content and services to users is well established, for example, as laid out in Federal Trade Commission Economic Issues paper on targeted online advertising.[18]

21. In sum, stated concern about privacy does not imply that consumers are harmed when they go online and data related to that activity is collected and used. Rather, that concern shows that consumers understand there to be a non-monetary tradeoff for the otherwise free content and services that they consume online. This tradeoff stems from understanding that their data may be used, understanding that that use occurs in ways that they do not understand or trust, and believing that they have little control over that use. In the face of that understanding, their actions in choosing to go online, to consume the free content and services that such use makes available, show that they believe that they benefit from that tradeoff.

B. Potential Consumer Privacy Harm Cannot be Presumed from Either a Common Mechanism or from Common Behaviors, Instead, to the Extent It Exists at All, Consumer Privacy Harm Varies Widely Depending on the Context and Consumers' Specific Preferences

22. In the context of privacy practices, such as those alleged by the Plaintiffs, the existence of a specific set of broadly applied practices—a common mechanism—does not imply a common injury because the context of where people may be exposed to those practices, and the framework and preferences of the people exposed to those practices, vary widely and substantially determine whether or how much they are harmed.

---

[16] *Ibid.*

[17] Garrett Johnson *et al*, *COPPAcalypse? The YouTube Settlement's Impact on Kids Content,* SSRN (2024) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4430334).

[18] Yan Lau, *A Brief Primer on the Economics of Targeted Advertising*, Federal Trade Commission: Bureau of Economics Economic Issues Paper (2020) (available at https://www.ftc.gov/reports/brief-primer-economics-targeted-advertising); *see also* Beales and Stivers, *An Information Economy Without Data*, SSRN (2022) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4279947).

23. As a conceptual matter, allegations of a privacy violation are about whether there is a flow of information related to a person that is contrary to that person's desire.[19] In this case, the Plaintiffs allege that TTI's practices with respect to its SDK and Events API resulted in such flows.

24. In some cases, alleging a common mechanism for injury could be enough to also allege, from a causal standpoint, that people were all harmed in a related way. For example, allegations of defective automobile brakes are, to frame it in a way that parallels allegations of a privacy violation, about whether a vehicle moved contrary to the driver's desire.

25. Less abstractly, drivers want to use their brakes to control the speed of their vehicle in order to avoid physical damage to property. A failure to control a vehicle that is caused by defective brakes results in damage that may be of varying degrees, but it provides the same basis for injury because the primary costs of fixing a car do not vary significantly according to the individual owner (e.g., how much they dislike driving, or whether they are looking for a job), or the context of the accident (e.g., they were going to work, or on a vacation).

26. In contrast, alleged privacy harms—harms stemming from an alleged failure to control the flow of information to be consistent with a person's desire—vary considerably by both the individual (according to their preferences and personal circumstances) and by the context (what kind of information is at issue, and where or why the information flowed). This idiosyncratic and contextual variation in the bases for privacy value or harm has been confirmed by the extensive literature on people's value of privacy as discussed in Section III.A.

27. For an illustration of the idiosyncratic nature of privacy value, consider the transmission of online activity data by ad networks. The primary use for the data transmitted to ad networks from website traffic is to be able to match relevant ads to interested viewers.[20] For example, a person interested in buying a new pair of sneakers may get more value

[19] *See* e.g. Economics of Privacy at 445.

[20] Note that no Plaintiff in any of the putative Classes would actually be exposed to a personalized ad due to the Defendant's alleged practices, they may attempt to argue that their (mistaken) *expectation* that the alleged data collection could result in an such an exposure caused them harm.

out of personalized ads that offer information on new deals or styles for them to consider over less relevant ads. Conversely, for the same personalized ad, some people might be annoyed by "receiving an unwanted email or advertisement."[21] This might be the case if an ad network receives data that a consumer has been shopping for sneakers, but not that the consumer has already made a purchase. This example also shows that the same person may value a personalized ad at one time, but not at another.

28. That heterogeneity in value can arise for more sensitive data, like religious affiliation, as well. While some people of a particular religion might appreciate personalized ads that match their interests, other people in that same religion may worry about the risk that information suggesting their affiliation would be breached or sold to someone that wishes them harm.[22] Still, others might simply dislike having their religious affiliation tracked at all, independent of any future outcome or effect.[23]

29. Each of these conceptual benefits, risks or costs could stem from the same data collection mechanism and privacy practices, but the nature and magnitude of any purported harm depends on the individual, their idiosyncratic situations, and their individual preferences. As noted in a seminal review on the economics of privacy: "privacy sensitivities and attitudes are subjective and idiosyncratic, because what constitutes sensitive information differs across individuals."[24]

30. These widely different and idiosyncratic privacy attitudes also mean that common behaviors that are intended to control the flow of personal information in some way do not imply that people would be harmed in the same way—or at all—if that control is breached.

31. For a contrasting example, the choice of a group of consumers to purchase fire insurance on their primary homes likely leads to a common injury if those purchases were fraudulent. The choice of purchasing fire insurance generally has one aim—to protect a physical and financial investment in the case of a fire. The choice of whether to use a

[21] See Danielle Citron and Daniel Solove, "Privacy Harms," *Boston University Law Review* 101 (2022) at 793-864 at 797. (available at https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf) (hereafter *Citron and Solove (2022)*.

[22] *Id.* at 839.

[23] *Ibid.*

[24] *See* Economics of Privacy at 446.

particular web service, or how to engage with various privacy controls provided by those services, is dependent on the idiosyncratic, and often unrelated, preferences and concerns of users.

32. In addition to the individual-specific future outcomes and preferences, perceived and potential privacy harms vary widely by context. The same review article cited above notes a theme of their review: "…is that characterizing a single unifying economic theory of privacy is hard, because privacy issues of economic relevance arise in widely diverse contexts." [25] Similarly, based on their review, they note that: "…the consequences and implications of data sharing or data protection vary very much with context—such as what specific type of data is being shared, how, and when."[26]

33. For example, some individuals may be more cautious and protective of personal information when using healthcare services,[27] as it could involve data that they may be more concerned about sharing. Conversely, many individuals find support and validation of their experience in being open about their healthcare challenges,[28] or may appreciate advertisements for products that help with those challenges. Similarly, consumers will be more cautious about financial transaction data as the consequences of losing control of that data may involve significant and concrete losses.[29] But here as well, the specific data at issue may cause some consumers to actively value sharing financial information.[30]

34. This general understanding by privacy researchers that broad claims of privacy value or harm cannot be distilled into a common framework has been acknowledged by legal scholars as well. Danielle Citron and Daniel Solove, both widely cited on privacy, note in their treatise on possible privacy harms that those harms may arise from many

[25] *Id.* at 443.

[26] *Id.* at 467.

[27] *See* Kim *et al*, "Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services," *Computers in Human Behavior* 92 (2019) at 273-281 (available at https://www.sciencedirect.com/science/article/pii/S0747563218305570).

[28] Campbell *et al*, "Cancer Peer Support Programs—Do They Work?" *Patient Education and Counseling* 55:1 (2004) at 3-15 (available at https://www.sciencedirect.com/science/article/pii/S073839910300301X?via%3Dihub).

[29] Juan Carrascal *et al*, *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online*, Cornell University (2011) (available at https://arxiv.org/pdf/1112.6098).

[30] *See e.g.*, Taylor Telford, "Younger women are practicing radical pay transparency on TikTok," *Washington Post* (July 6, 2024) (available at https://www.washingtonpost.com/business/2024/07/04/young-women-pay-transparency-tiktok/).

different sources and at different stages of possibility: "Courts struggle with privacy harms because they often involve future uses of personal data that vary widely."[31] That work lists seven separate potential bases for potential privacy harm: physical, economic, reputational, psychological, autonomy, discrimination, and relationship harms.

35. Overall, the empirical research, as well as the more general literature around privacy values and harm emphasizes the variability in contexts and preferences. What is more, the differences in context need not be large in order to drive large differences in value. The wide range of measured harms or values in privacy research shows that "small changes in contexts and scenarios can lead to widely differing conclusions regarding consumers' willingness to pay to protect their data."[32] These "small changes in context" are both clear and common across the websites cited by the Plaintiffs, and in many cases those changes are more than small.

C. Privacy Policies Vary Widely Across Websites, and Consumers Vary Widely in Terms of Their Understanding of Those Privacy Policies

36. In fact, we see significant changes in context, including in the privacy controls and policies that individual websites choose to implement. As alleged in the Second Amended Complaint, there are hundreds of thousands of websites[33] that have chosen to use TTI's SDK with Pixel. As the complaint illustrates, these websites cover nearly the full range of services and content available on the internet.

37. For example, Hulu is a subsidiary of a major media company with a comprehensive and sophisticated approach to privacy that is tailored to its audience, including both adults and children.[34] Build-a-Bear, as a seller of products desired by children, but typically purchased by adults, also has particular needs, and particular policies that are unique to its need to ensure that it does not violate the Childrens Online Privacy and Protection Act.[35] Rite Aid, as a retail store that also sells pharmacy services tailors its policy and

[31] *See Citron* and Solove (2022) at 793.

[32] *See* Acquisti *et al* (2016) at 479.

[33] *See* Second Amended Complaint ¶ 59.

[34] "Privacy Policy," *Walt Disney Privacy Center* (available at https://privacy.thewaltdisneycompany.com/en/current-privacy-policy/) (accessed at 6/24/2024).

[35] "Build-A-Bear Workshop Global Privacy Policy," *Stuffed Animals, Plush and Teddy Bears* (available at https://www.buildabear.com/privacy-policy.html) (accessed at 6/24/2024).

choices to adults, but also includes special considerations for protection of patient privacy and health data.[36] Etsy, as a market platform, has to tailor its privacy policies and controls to meet the needs of both its sellers and its buyers.[37] Each of the other websites that use the TikTok Pixel will similarly have unique needs and approaches to privacy depending on their audience, the services they provide, and the regulatory requirements for the jurisdictions of their consumers.

38. Users also have a variety of approaches to assessing how these websites might affect their privacy preferences. Research has shown that when different consumers are asked to read privacy policies carefully, they differ in their interpretation of what the privacy notices authorize.[38] Readers of the policies tend to project their own expectations and notions of privacy onto the notices. Moral intuitions, context, social norms, and experience have also been found to play an important role in how consumers understand policy notices.[39] All of these factors are likely to vary considerably across the relevant websites for each user.

39. In addition, users vary by whether they read a privacy policy, even when they say that they are concerned about privacy. Over half of Americans "almost always or often" click "agree" right away, without reading what privacy policies say.[40] That is, even when a website "requires" consumers to read the policy, many do not. Even among

[36] "Online Privacy & Security Policy," *Rite AID* (available at https://www.riteaid.com/legal/privacy-policy) (accessed at 6/24/2024).

[37] "Privacy Policy – Our House Rules," *Etsy* (available at https://www.etsy.com/legal/privacy/) (accessed at 6/24/2024).

[38] Kirsten Martin, "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying With a Privacy Notice is Related to Meeting Privacy Expectations Online," *SSRN* (2014) at 2 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2518581) ("Perhaps most problematic, respondents projected the important factors of their privacy expectations onto the privacy notice.").

[39] Lior Strahilevitz and Matthew Kugler, "Is Privacy Policy Language Irrelevant to Consumers?" *The Journal of Legal Studies* 45(2) (2016) at S69-S95 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449). ("Context, experience, and norms, rather than privacy policy language, seem to benchmark consumers' understandings about what conduct they are authorizing."); *see also* Tess Wilkinson Ryan, "Legal Promise and Psychological Contract," Wake Forest Law Review 47 (2012) 843-873 at 845 (available at https://wakeforestlawreview.com/wp-content/uploads/2014/10/Wilkinson-Ryan_LawReview_1.13.pdf). ("Furthermore, empirical research on informal norms in legal decision making has yielded evidence that people draw on a set of consistent moral intuitions and social norms to understand the substance of the promissory obligation.").

[40] Colleen McClain *et al*, *How Americans Protect their Online Data*, Pew Research Center (October 2023) (available at https://www.pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/) (hereafter *McClain (2023)*); *see* also Auxier (2019) at 4. ("Fully 97% of Americans say they are ever asked to approve privacy policies, yet only about one-in-five adults overall say they always (9%) or often (13%) read a company's privacy policy before agreeing to it. Some 38% of all adults maintain they sometimes read such policies, but 36% say they never read a company's privacy policy before agreeing to it.").

consumers who say they are most concerned about privacy, nearly half of those admit to "almost always or never" reading the policy.[41] This reflects that most people understand the transaction that occurs when you go online.

D. Consumers Use a Wide Variety of Tools to Minimize or Prevent Tracking of Online Activity

40. Along with their varying preferences, concerns, and engagement with websites' privacy policies, consumers can use, or not, a variety of privacy tools—each with their own level and scope of protection against potential harms. These tools include choices at the device level (e.g., Android, iOS, MacOS, Windows), at the browser level, and for individual sites or platforms.[42] Privacy tools are also available from for profit[43] or non-profit[44] entities in the form of overall privacy plans, plug-ins to browsers or as device level tools.

41. The use of these tools is widespread, but consumers engage with these tools to varying degrees. For example, the Pew Research Center found that two-thirds of American adults "have declined or turned off cookies or other tracking on websites."[45] The survey found that close to half of American adults chose a browser or search engine to avoid tracking.[46] Both of those behaviors were found to vary by age and education.[47] As noted in Section III.B., users' concern about privacy, and the potential harms that they might consider varies by context. This variation is likely to also drive variation in engagement with various privacy tools by the same person.

42. This variation in use of tools and other online practices, like the variation in concerns, matters here because the degree to which a person's choices about the available tools

---

[41] *Ibid.*

[42] *See* e.g. U.K Competition & Market Authority, *Online Platforms and Digital Advertising Market Study, Appendix K,* (July 1, 2020) at ¶¶8 (available at https://assets.publishing.service.gov.uk/media/5fe49595d3bf7f089f9998ce/Appendix_K_-_consumer_controls_over_platforms__data_collection_WEB.pdf).

[43] *See e.g.* various products from the security firm Norton. *See* Protection for Your Digital Age, *Norton* (available at https://buy-static.norton.com/norton/ps/bb/ushard/360/us_en_nort_brfr-ft30.html) (accessed at 7/7/2024).

[44] *See e.g.* Security Planner, *Consumer Reports* (available at https://securityplanner.consumerreports.org/) (accessed at 7/7/2024); *see also* Privacy Badger, *Electronic Frontier Foundation* (available at https://privacybadger.org/) (accessed at 7/7/2024) (hereafter *EFF Privacy Badger)*.

[45] McClain (2023) (*See section* "How People are Protecting their Digital Privacy").

[46] *Ibid.*

[47] *Ibid.*

blocks the transmission of information to third parties like TTI, will determine whether, or how much that person *could* be harmed by such practices.

43. However, that variation in concern also means that the use, or degree of use, of privacy tools or behaviors does not determine the magnitude of any such harm because the motive for doing so could vary significantly. One user might employ a tracking blocker because they dislike ads, independent of whether they were being tracked,[48] such that they would perceive no harm from tracking. Other users might be most interested in not being tracked. But even in this case, why they wanted not to be tracked matters for determining any alleged harm.

44. In sum, the preferences and behaviors of American adults have been found to vary widely. Those idiosyncratic and contextual preferences and behaviors will determine whether, and, if so, how much, any alleged data collection and use practices could harm any individual online user.

E. The Named Plaintiffs' Privacy Harms and Online Practices are Idiosyncratic and Context Dependent

45. The complaint alleges facts about three Plaintiffs with regard to their privacy concerns, preferences and harms. For none of the Plaintiffs does the complaint specify a privacy concern for why they may have avoided registering as TikTok users. However, the complaint and the depositions do indicate that each of the three is alleging a different basis for such privacy concerns.

46. For example, in the Complaint, Ms. Shih is said to be a consultant for the Florida Department of Transportation, where she works with confidential material, with the implication that she may be concerned about losing her job if confidential data is breached.[49] Mr. Watters is said to have been a user of Upwork, which connects freelance workers with employers.[50] Here, given that he was presumably sharing personal data in an attempt to be employed, it is unclear whether the complaint is alleging a privacy harm related to that website. Finally, Ms. Griffith is presented as a general web user,

[48] In many cases ad blocking is bundled with blocked tracking. *See, e.g., EEF Privacy Badger (see FAQ "Why does Privacy Badger block ads?").*

[49] *See* Second Amended Complaint ¶ 117.

[50] *See* Second Amended Complaint ¶ 132.

having visited a variety of sites, but no specific background is alleged that provides a specific privacy issue.[51]

47. Privacy researchers and advocates agree that privacy concerns arise from a range of possible activities, outcomes and values. Those values that users place on giving or withholding access to data about them conceptually stem from a broad range of possible sources. And those values could be either positive or negative, depending on the individual and the context.

48. Evaluating any alleged privacy harm to each of the plaintiffs would require a separate framework, data, and analysis. Each analysis would result in unrelated estimations of harm. For example, analyzing any harm stemming from exposure of work data to Ms. Shih would require understanding her pay, her liability should confidential data be breached, and her other opportunities for work.

49. Evaluating harm to Ms. Griffith may require estimating her allegedly very high intrinsic value of privacy. Different from that of Ms. Shih, where an evaluation of their harm could potentially be linked to the risk of a concrete outcome, Ms. Griffith's alleged harm could be ungrounded, and unbounded. The alleged privacy harm to Mr. Watters from his online activity cannot be characterized based on the information in the complaint. Likely, it would be as subjective as the way Ms. Griffith "intrinsically" may value her privacy. Because these intrinsic values are completely idiosyncratic, and generally not informed by any relevant market or concrete outcome, they are unlikely to stem from the same calculation or source of concern. Finally, many companies provide pixels, or related technologies to websites that choose to implement them and potentially transmit information to an ad network.[52]

50. Additional plaintiffs will undoubtedly have similar idiosyncratic subjective valuations, and contexts that make any unified analysis of harm impossible, consistent with the consensus of researchers in the field. The technologies, preferences, contexts and

[51] *See* Second Amended Complaint ¶¶ 107-115.

[52] Todd Feathers *et al,* ""Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies," *The Markup* (December 13, 2022) (available at https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies).

behavior of each plaintiff will vary widely, and that variance will drive wide variance in the frameworks underlying any alleged harm.

51. Indeed, during depositions of the named Plaintiffs, [redacted][53] [redacted][54] [redacted][55] [redacted][56] [redacted][57] [redacted][58] [redacted][59] [redacted]

52. In terms of [redacted] each of the named Plaintiffs [redacted][60] [redacted][61] [redacted]

[53] *See* Deposition of Patricia Shih Blough (June 27, 2024) at 130.

[54] *Id.* at 183-185.

[55] *Id.* at 127.

[56] *See* Deposition of Jacob Leady (June 25, 2024) at 51, 240-41.

[57] *Id.* at 106.

[58] *Id.* at 204.

[59] *See* Deposition of Bernadine Griffith (June 26, 2024) at 89-90.

[60] *Id.* at 92.

[61] *Id.* at 146-48.

[redacted][62]

[redacted][63]

[redacted][64]

53. Each of the named Plaintiffs also [redacted][65]

[redacted][66]

[redacted][67]

[redacted][68]

[redacted][69]

[redacted][70]

[redacted][71]

54. Each of the Plaintiffs is also alleged to have been harmed by the diminution of the value of their data, as they speculate it could be sold through their participation in surveys or focus groups. First, as noted by leading privacy researcher Catherine Tucker, "[t]here are plenty of firms who have sought to set up businesses which would allow individuals to own their data and trade it for monetary value… However, as of yet none of these

[62] *See* Deposition of Patricia Shih Blough (June 27, 2024) at 183-91.

[63] *Id.* at 92-103.

[64] *See generally* Deposition of Jacob Leady (June 25, 2024).

[65] *Id.* at 76.

[66] *Id.* at 91.

[67] *See* Deposition of Patricia Shih Blough (June 27, 2024) at 167.

[68] *Id.* at 164.

[69] *Id.* at 161.

[70] *See* Deposition of Bernadine Griffith (June 26, 2024) at 130.

[71] *See id.* at 132.

efforts have thrived."[72] That is, there is little evidence that individuals can sell their data as a substitute for web tracking. At least one of the named Plaintiffs [redacted][73]

55. Instead, the purpose and use of data collected through surveys and focus groups is quite different from data collected through website tracking tools from ad networks. Based on my work and research, I am not aware of any significant overlap in these markets for data. In connection with this assignment, I have looked for research or other evidence that might substantiate Plaintiffs' theory that there is a market for data as they describe, and I have found none. Because the markets Plaintiffs identify are unlikely to exist, or to be substitutes for the data collection alleged by the Plaintiffs, there is no reason to believe that one would significantly diminish the other. In addition, I understand that TTI does not use or sell non-TikTok user data for any purpose. This means that even if the allegedly collected data itself was substitutable, it would not have been available as a substitute.

56. As evidence that such panel data is not considered a substitute for the data collection alleged here, note that Google's terms of service for its Screenwise panel does not include any exclusive license to such web-browsing data.[74] In fact, it appears to explicitly contemplate the parallel collection of data by other parties by noting that it will track the cookies that appear on panelists devices and applications.[75] That is, there is no plausible diminution in value to the Plaintiffs caused by a market substitution that does not exist.

57. Finally, note that all the named Plaintiffs indicate that [redacted]

[72] Catherine Tucker, "The Economics of Privacy: An Agenda," *National Bureau of Economic Research* (2023) at 11 (available at https://www.nber.org/system/files/chapters/c14781/c14781.pdf); *see* also Economics of Privacy at 447.

[73] *See* Deposition of Patricia Shih Blough (June 27, 2024) at 335.

[74] "Google Panel Privacy Policy," *Screenwise* (available at https://screenwisepanel.com/google-panel-privacy-policy) (accessed at 6/24/24).

[75] *Id. (*"Cookies, unique numbers, or other identifiers from your browser, applications, or device, including anonymous and pseudonymous identifiers as well as cookies or other identifiers associated with your personal information or Google Account(s).")

[redacted][76] [redacted]

[redacted][77] [redacted]

[redacted]

[redacted][78] [redacted]

[redacted][79] [redacted]

[redacted]

[redacted]

[redacted]

58. Mr. Watters provided [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted][80] [redacted]

[redacted]

[redacted]

[redacted][81] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

59. Second, Mr. Watters testified [redacted]

[redacted]

[redacted][82] [redacted]

[redacted]

[76] See Deposition of Patricia Shih Blough (June 27, 2024) at 79.

[77] *Id.* at 123, *see also* 169 ([redacted]).

[78] *Id.* at 292.

[79] *See* Deposition of Bernadine Griffith (June 26, 2024) at 254.

[80] *See* Deposition of Jacob Leady (June 25, 2024) at 91. See also at 94, in response to the question, [redacted]

[redacted]

[81] *Id.* at 284.

[82] *Id.* at 331.

[redacted] While as noted above in Section III.A. people's stated intentions often differ from their actions, [redacted]

60. In sum, even across only these three Plaintiffs there is a wide range of potential motivations and interests that would determine the framework for evaluating any harms from the advertisers' use of the TikTok Pixel and Events API. I understand that the Plaintiffs more broadly are contemplating a class that would include all internet users who visited a range of at least hundreds of thousands of websites across more than two years. The range of different frameworks for valuing privacy—including preferences, behaviors, and contexts—across the users of the internet, even excluding the numerous TikTok users, will cover the full and varied range in the U.S. adult online population, as documented in the studies and reviews discussed above. In addition, narrowing the class by geography (to California) or by behavior (to those using cookie blockers) will not by itself provide a unifying framework.

61. As noted above, most Americans articulate general privacy concerns, that are not tied to a particular company. In a 2021 survey of Americans[83] that asked the open-ended question "What is your biggest privacy concern?," out of 3,338 responses, 88 percent either expressed no concern, or fit into one of eight broad categories of concern.[84] The author reports that a small group of additional themes, one of which was reported as concern about "social media," came up "between 0.6 percent and 1.3 percent of total responses".[85] That is, research does not support the idea that avoidance of TikTok is a general motivating force behind privacy concerns, or potential harm from privacy violations.

[83] Jim Harper, *What Do People Mean by "Privacy," and How Do They Prioritize Among Privacy Values? Preliminary Results*, American Enterprise Institute (March 2022) (available at https://www.aei.org/research-products/report/what-do-people-mean-by-privacy-and-how-do-they-prioritize-among-privacy-values-preliminary-results/).

[84] *Id.* at 3.

[85] *Ibid.*

I declare under the penalty of perjury that the foregoing is true and correct. Executed this 12th day of July, 2024, in Bethesda, Maryland.

Stivers, Andrew

Digitally signed by Stivers, Andrew
Date: 2024.07.12 06:14:48 -04'00'

Andrew Stivers

APPENDIX I:
CV of Andrew Stivers, PhD

ANDREW STIVERS
Managing Director

Overview

Dr. Andrew Stivers is one of the world's leading experts in consumer protection economics, having spent 7 years heading the U.S. Federal Trade Commission's consumer protection economics work – designing, implementing and evaluating complex economic and survey analyses of the Commission's enforcement and policy matters. Dr. Stivers specializes in novel and complex questions of consumer behavior and damages related to unfairness, deception, privacy, data security, algorithmically driven practices, and cutting edge promotion and advertising strategies.

Dr. Stivers' has provided his economic expertise to companies in the top tiers of the media streaming, retail platform, AI, gig economy, gaming, and health data industries. He has also advised a broad range of both established and growing businesses, including in the ultra-high-end luxury goods, telecommunications, payments, investment, and food/supplement industries. Dr. Stivers has experience in federal and state enforcement and policy as well as private Lanham Act and class action matters, including acting as an expert witness. Dr. Stivers also provides ability-to-pay analyses in the context of monetary remedy negotiations.

Prior to joining NERA, Dr. Stivers was a senior official in the US Federal Trade Commission's Bureau of Economics, where he oversaw economic analysis of all consumer protection and privacy matters. He advised the Bureau of Consumer Protection and FTC Commissioners on hundreds of regulatory and law enforcement matters during his seven-year tenure leading this work at the Commission.

Prior to his leadership role at the FTC, Dr. Stivers served as the Director of the Division of Public Health Informatics and Analytics at the Food and Drug Administration's Center for Food Safety and Applied Nutrition. In that role, he oversaw the Center's statistical, epidemiological, and consumer research groups. His regulatory work for the agency included providing economic and behavioral analysis to consumer nutrition labeling initiatives. Prior to joining the Federal government, as an academic, Dr. Stivers focused his research on the regulation of information and language in the marketplace.

Dr. Stivers has written and presented on complex and wide-ranging economic topics, published economic papers, and presented keynotes and panel discussions on a variety of informational, privacy, data security, and consumer behavior topics. These include invited presentations at academic, practitioner and regulator-sponsored conferences, including by the FTC, the ABA and the Bank of Canada.

Current Position

Managing Director, NERA Economic Consulting
2024-present

Education

Ph.D. in economics, University of Texas at Austin
M.A. in economics, University of Texas at Austin
B.A. in history with honors, University of Texas at Austin

Recent Professional Experience

Director, NERA Economic Consulting
2021-2023

Deputy Director for Consumer Protection, Bureau of Economics, US Federal Trade Commission
2014-2021

Director, Division of Public Health Informatics and Analytics, Center for Food Safety and Applied Nutrition, US Food and Drug Administration
2011-2014

Honors and Professional Activities

Co-Chair, Economics Committee, Antitrust Section ABA 2024-present

Vice-Chair, Consumer Protection Committee, Antitrust Section ABA 2021-2024

Member American Economic Association

Publications

"The Impact of Colorado Ending Equal Competition between State and National Banks" (with Howard Beales) *SSRN working paper*, October 2023.

"Generative AI and Guidance on Abusiveness May Illuminate a New Focus on "Dark Patterns" for Enforcement and Related Consumer Research" *The Antitrust Source* August, 2023.

"The War on So-Called 'Junk Fees': Who's Fighting and What's at Stake?" (with Donnelly McDowell) *CPI Antitrust Chronicle*, April, 2023.

"An Information Economy Without Data" (with Howard Beales), *SSRN working paper,* December 2022.

"The Algorithmic Accountability Act: Potential Coverage Gaps in the Healthcare Sector" (with Maneesha Mithal and Gabriela Monahova) *Antitrust Magazine Online*, August, 2022.

"How The FTC Is Imposing Monetary Remedies Post-AMG" *Law360*, July 2022.

"Novel Privacy Concerns in Healthcare Antitrust" with Emily Walden and Subramaniam Ramanarayanan *CPI Antitrust Chronicle* May 2022.

"For The CFPB, Evaluating 'Junk Fees' May Be Complicated" Law360, March 2022.

"What FTC Report Reveals About ISP Data Collection" *Law360*, December 2021.

"Proposed FTC Rulemaking: "Simply" Section 5 deception, but with penalties?" *LinkedIn*, October 2021.

"Monetary Remedies for Zero-Price Privacy Regulation." *CPI Antitrust Chronicle*, September 2021.

"Monetary Remedies After High Court FTC Ruling." *Law360*, August 2021.

"Regulatory lessons from FTC's MUSA rulemaking: Does existing enforcement policy mean costless rules?" *LinkedIn*, July 2021.

"An Extension of Train (2015): Welfare Calculations in Discrete Choice Models When Anticipated and Experienced Attributes Differ, and When Market Attributes and Price May Be Conditional on Whether Consumers Are Misled." *SSRN Working Paper*. December 2019.

"The Alchemy of a Pyramid: Transmutating Business Opportunity into a Negative Sum Wealth Transfer." with Douglas Smith and Ginger Zhe Jin. *SSRN Working Paper.* December 2019.

"Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics," with Ginger Zhe Jin, *SSRN Working Paper*. 2017.

"Voluntary Quality Disclosure under Price-Signaling Competition" with Fabio Caldieraro and Dongsoo Shin. *Managerial and Decision Economics* 32(8) 493-504. 2011

"Pricing in Retail Gasoline Markets." with Scott Russell, Starr McMullen and Santosh Mishra. *Journal of the Transportation Research Forum* 49(2) Summer Issue. 2010.

"Regulating Market Language: Market Failure in Descriptive Signals." *Journal of Consumer Policy* 32(1) 23-41. 2009

"Same Sex Marriage and the Regulation of Language." with Andrew Valls. *Politics, Philosophy and Economics* 6(2) 237-253. 2007.

"Language Regulation and Dissipation in Meaning." *Proceedings, Workshop on Language, Games and Evolution, 19th European Summer School in Logic, Language and Information*. Dublin. 2007

"Optimal Number of Standards under Economies of Scope in Quality Production." *Economics Letters* 90(3) 368-372. 2006.

"Advertising, Search Costs, and Social Welfare." with Victor Tremblay. *Information Economics and Policy* 17(3) 317-333. 2005

"Unraveling of Information: Competition and Uncertainty." *Topics in Theoretical Economics* 4(1) 9. 2004.

"Quality Standards with Exogenously Distributed Quality." *Economics Letters* 80(1): 131-136. 2003.

Presentations and Speeches

"2023 Privacy Update: FTC, Congress, and the States" Webinar Panelist. Program on Economics and Privacy (with James Cooper, Maneesha Mithal and Adam Kovacevich), Law and Economics Center, George Mason University June 2023.

"Dark Patterns: New Work, Emerging Solutions" (moderator) 2023 Antitrust Law Section Consumer Protection & Data Privacy Conference, February 2023.

"Round-Up on Consumer Protection and Privacy Trends" 2022 ABA Antitrust Law Section In-House Institute, September 2022.

"Economics of Competition and Consumer Protection: Complements?" (with James Cooper and Bruce Kobayashi) Tenth Annual Symposium on the Law & Economics of Privacy & Data Security, June 2022.

"Consumer Protection and Algorithmic Bias" (with Lauren Aronson (Corwell & Moring) and Vikram Swaruup (DC AG's Office)) ABA Consumer Protection Committee Panel, June 2022.

"FTC Warning Letters: What are they and what's next" (with Lauren Aronson (Corwell & Moring), David Vladeck (Georgetown Law) and Mike Sherling (Perkins Coie)) ABA Consumer Protection Committee Webinar, November, 2021.

"Claim Substantiation and Advertising Perception Surveys" (with Melissa Pittaoulis (NERA) and Mary Engle (BBB National Programs)) Survey Evidence in Litigation Series, NERA Economic Consulting Webinar, October 2021.

"FTC's Revolution Through Rulemaking" (with Corbin K. Barthold (TechFreedom), William Blumenthal (Sidley Austin) and Svetlana Gans (NCTA)) Regulatory Transparency Project Webinar, October 2021

"Economics Where Privacy Meets Big Data" (with Alexei Alexandrov (Wayfair), Rachel Marmor (Davis Wright Tremaine), and Ling Ang (NERA)). ABA Section of Antitrust Law Webinar, January 2021.

"FTC Remedial Authority: Powers, Process, and Suggestions for Reform" (with

James Cooper (Scalia Law School), Svetlana Gans (NCTA), Berin Szóka (TechFreedom) and John Villafranco (Kelly, Drye & Warren)) Regulatory Transparency Project Teleforum, June 2020.

"Protecting Consumers in Privacy and Data Security," Invited Presentation for the Bank of Canada Annual Conference: Learning about the Digital Economy. Ottawa, Canada. November 2019.

"Practices, Outcomes, Injury and Risk," Keynote for the Third Annual Digital Information Policy Scholars Conference. 2018.

Closing Remarks, Informational Injury Workshop, U.S. Federal Trade Commission. 2017.

"Basic Economics of Privacy," Third Annual LEC Public Policy Conference on Privacy and Data Security. Arlington VA. 2015.

"More Than You Wanted to Know: The Failure of Mandated Disclosure." (with Paul S. Atkins (Patomak Global Partners), Omri Ben-Shahar (U Chicago) and Thaya Brook Knight (Cato Institute) Book Event Co-sponsored by the Federalist Society Faculty Division and the Cato Institute. 2015.

"Privacynomics: The Proper Role of Economics in Privacy Policymaking," (with Mark Brennan (Hogan Lovells) and James Cooper (Scalia Law School)) IAPP Global Privacy Summit 2015. Washington, DC. 2015.

"Behaviorally-Informed Approaches to Risk Regulation." Introduction to Behavioral Economics Workshop, Society for Risk Analysis Annual Meeting Salt Lake City, December 2010.

Appendix II:
Materials Considered

1. Brooke Auxier *et al*, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 2019) (available at https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf).
2. Alessandro Acquisti *et al*, "The Economics of Privacy," *Journal of Economic Literature* 54(2) (2016) 442-492 (available at *http://doi.org/10.1257/jel.54.2.442*). (hereafter *Economics of Privacy*).
3. Colleen McClain *et al*, *Views of Data Privacy Risks, Personal Data and Digital Privacy Laws*, Pew Research Center (October 2023) (available at https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/).
4. "Internet, Broadband Fact Sheet," *Pew Research Center* (January 2024) (available at https://www.pewresearch.org/internet/fact-sheet/internet-broadband/) (accessed 6/17/2024).
5. Andrew Perrin and Sara Atske, "About three-in-ten U.S. Adults say they are 'Almost Constantly' Online," *Pew Research Center* (March 2021) (available at https://www.pewresearch.org/short-reads/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/).
6. NTIA, "Most popular online activities of adult internet users in the United States as of November 2021," *Statista* (available at https://www.statista.com/statistics/183910/internet-activities-of-us-users/) (accessed at 6/27/24).
7. Daniel J Solove, "The Myth of the Privacy Paradox," *George Washington Law Review* 89 (2021) 1-51 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265).
8. Susan Athey *et al,* "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," *National Bureau of Economic Research* (2017) (available at https://www.nber.org/papers/w23488).
9. Icek Ajzen *et al,* "The Influence of Attitudes on Behavior," in Dolores Albarracin *et al* eds., *The Handbook of Attitudes Volume 1: Basic Principles* (New York, NY: Routledge, 2019) (available at https://people.umass.edu/aizen/pubs/aonb.pdf).
10. Patrick Pelsmacker *et al*, "Do Consumers Care about Ethics? Willingness to Pay for Fair-Trade Coffee," *Journal of Consumer Affairs* 39(2) (2005) at 361–383 (available at https://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2005.00019.x).
11. Jens Hainmueller *et al*, "Consumer Demand for Fair Trade: Evidence from a Multistore Field Experiment," *Review of Economics and Statistics* 97(2) (2015) at 242-256 (available at https://web.stanford.edu/~jhain/Paper/REST2015.pdf).
12. Erik Brynjolfsson *et al*, "The Digital Welfare of Nations: New Measures of Welfare Gains and Inequality," *National Bureau of Economic Research* (2023) (available at https://www.nber.org/papers/w31670).
13. Yan Lau, *A Brief Primer on the Economics of Targeted Advertising*, Federal Trade Commission: Bureau of Economics Economic Issues Paper (2020) (available at https://www.ftc.gov/reports/brief-primer-economics-targeted-advertising).

14. See Danielle Citron and Daniel Solove, "Privacy Harms," *Boston University Law Review* 101 (2022) at 793-864 at 797. (available at https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf).
15. Kim *et al*, "Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services," *Computers in Human Behavior* 92 (2018) at 273-281 (available at https://www.sciencedirect.com/science/article/pii/S0747563218305570).
16. Juan Carrascal *et al*, *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online*, Cornell University (2011) (available at https://arxiv.org/pdf/1112.6098).
17. "Privacy Policy," *Walt Disney Privacy Center* (available at https://privacy.thewaltdisneycompany.com/en/current-privacy-policy/) (accessed at 6/24/2024).
18. "Build-A-Bear Workshop Global Privacy Policy," *Stuffed Animals, Plush and Teddy Bears* (available at https://www.buildabear.com/privacy-policy.html) (accessed at 6/24/2024).
19. "Online Privacy & Security Policy," *Rite AID* (available at https://www.riteaid.com/legal/privacy-policy) (accessed at 6/24/2024).
20. "Privacy Policy – Our House Rules," *Etsy* (available at https://www.etsy.com/legal/privacy/) (accessed at 6/24/2024).
21. Kirsten Martin, "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying With a Privacy Notice is Related to Meeting Privacy Expectations Online," *SSRN* (2014) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2518581).
22. Lior Strahilevitz and Matthew Kugler, "Is Privacy Policy Language Irrelevant to Consumers?" *The Journal of Legal Studies* 45(2) (2016) at S69-S95 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449).
23. Tess Wilkinson Ryan, "Legal Promise and Psychological Contract," Wake Forest Law Review 47 (2012) 843-87 (available at https://wakeforestlawreview.com/wp-content/uploads/2014/10/Wilkinson-Ryan_LawReview_1.13.pdf).
24. Colleen McClain *et al*, *How Americans Protect their Online Data*, Pew Research Center (October 2023) (available at https://www.pewresearch.org/internet/2023/10/18/how-americans-protect-their-online-data/).
25. Catherine Tucker, "The Economics of Privacy: An Agenda," *NBER* (2023) at 11 (available at https://www.nber.org/system/files/chapters/c14781/c14781.pdf).
26. "Google Panel Privacy Policy," *Screenwise* (available at https://screenwisepanel.com/google-panel-privacy-policy) (accessed at 6/24/24).
27. *See* "SavvyConnect FAQs," SurveySavvy (available at https://surveysavvy.com/savvyconnect-faqs/) (accessed 6/25/24).
28. "Ipsos Screenwise Panel Cookie Policy," Ipsos (available at https://screenwisepanel.com/cookie-policy) (accessed 6/25/24).
29. "Computer & Mobile Panel," Nielsen (available at https://computermobilepanel.nielsen.com/ui/US/en/sdp/land) (accessed 6/25/24).
30. Jim Harper, *What Do People Mean by "Privacy," and How Do They Prioritize Among Privacy Values? Preliminary Results*, American Enterprise Institute (March 2022) (available at https://www.aei.org/research-products/report/what-do-people-mean-by-privacy-and-how-do-they-prioritize-among-privacy-values-preliminary-results/).
31. Veronica Marotta *et al*, "The Welfare Impact of Targeted Advertising Technologies," *Information Systems Research* 33(1) (2022) 131-151 (available at https://doi.org/10.1287/isre.2021.1024).

32. "The World's Most Valuable Resource is No Longer Oil, But Data," *The Economist* (May 2017) (available at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data).
33. Tim O'Reilly, "Data Is the New Sand," *The Information* (February 2021) (available at https://www.theinformation.com/articles/data-is-the-new-sand).
34. Garret Johnson *et al*, "Consumer Privacy Choice in Online Advertising: Who Opts out and at What Cost to Industry?" *Marketing Science* 39(1) (2020) 33-51 (available at https://doi.org/10.1287/mksc.2019.1198).
35. Hal Varian, Intermediate Microeconomics with Calculus, 1st. ed. (New York: WW Norton & Company, 2020).
36. Queirolo *et al, "*The Role of Economics in Bycatch Valuation," *Institute of Social and Economic Research* (1980) (available at https://scholarworks.alaska.edu/handle/11122/14370).
37. Declaration of Russell W. Magnum III (June 21, 2024).
38. Declaration of Zubair Shafiq (June 21, 2024).
39. Second Amended Class Action Complaint (April 11, 2024).
40. Defendants TikTok Inc. and Bytedance Inc.'s Answer to Platiffs' Second Amended Complaint.
41. 2024-4-16 Defendants' Amended R' Second Set of Interrog (Nos. 3-14).pdf (April 22, 2024).
42. Joseph Turow *et al, Americans Can't Consent to Companies' Use of Their Data: They Admit They Don't Understand It, Say They're Helpless to Control It, and Believe They're Harmed When Firms Use Their Data--Making What Companies Do Illegitimate,* University of Pennsylvania Annenberg School of Communication (2023) (available at https://ssrn.com/abstract=4391134).
43. Lorrie Cranor *et al*, *Beyond Concern: Understanding Net User' Attitudes about Online Privacy*, Massachusetts Institute of Technology (1999) (available at https://arxiv.org/abs/cs/9904010).
44. Dube *et al*, "The Intended and Unintended Consequences of Privacy regulation for Consumer Marketing," *Marketing Science Institute* (2024) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4847653).
45. David Fehrenbach and Carolina Herrando, "The Effect of Customer-Perceived Value When Paying for a Product with Personal Data: A Real-Life Experimental Study," *Journal of Business Research* Vol. 137 (2021) 222-232 (available at https://www.sciencedirect.com/science/article/pii/S0148296321005907).
46. Timothy Graeff and Susan Harmon "Collecting and using personal data: consumers' awareness and concerns", *Journal of Consumer Marketing* 19(4) (2002) 302-318 (available at http://dx.doi.org/10.1108/07363760210433627).
47. Ginger Zhe Jin and Andrew Stivers, *Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics* (2017) (available at https://ssrn.com/abstract=3006172).
48. H. Li and A. Nill, "Online Behavioral Targeting: Are Knowledgeable Consumers Willing to Sell Their Privacy?" *Journal of Consumer Policy* 43 (2020) 723–745 (available at https://doi.org/10.1007/s10603-020-09469-7).
49. Tesary Lin and Avner Strulov-Shlain, *Choice Architecture, Privacy Valuations, and Selection Bias in Consumer Data*, University of Chicago (2023) (available at https://bfi.uchicago.edu/working-paper/choice-architecture-privacy-valuations-and-selection-bias-in-consumer-data/).
50. Paul Slovic, "Perception of Risk" (1987) (available at https://pages.ucsd.edu/~aronatas/project/academic/risk%20slovic.pdf).

51. Tess Wilkinson-Ryan, *Moral Judgment and Moral Heuristics in Breach of Contract*, Journal of Empirical Legal Studies 407 (2009) (available at https://scholarship.law.upenn.edu/faculty_scholarship/2573)
52. Jan Schumann *et al,* "Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance Among Users of Free Web Services," *SSRN* (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2351777).
53. Defendants TikTok Inc. and Bytedance Inc.'s Notice of Motion and Motion to Dismiss Plaintiff's First Amended Complaint (November 8, 2023).
54. Defendants TikTok Inc. and Bytedance Inc.'s Reply in Support of Motion to Dismiss Plaintiff's First Amended Complaint (December 12, 2023).
55. Pew Research Center, *The Internet's Value in Everyday Life: Americans Admire it and Find it a Useful Tool* (June 28, 2024) (available at https://www.pewresearch.org/internet/2004/08/11/part-2-the-internets-value-in-everyday-life-americans-admire-it-and-find-it-a-useful-tool/).
56. Plaintiff's Memorandum of Points and Authorities in Support of Their Motion for Class Certification (June 21, 2024).
57. John Boyce, "An Economic Analysis of the Fisheries Bycatch Problem", *Journal of Environmental Economics and Management* 3,1996(31) (1996) 314-336 (available at https://doi.org/10.1006/jeem.1996.0047).
58. Colleen McClain *et al*, *How Americans Navigate Politics on TikTok, X, Facebook and Instagram*, Pew Research Center (June 12, 2024) (available at https://www.pewresearch.org/internet/2024/06/12/how-americans-navigate-politics-on-tiktok-x-facebook-and-instagram/).
59. Garrett Johnson *et al*, *COPPAcalypse? The YouTube Settlement's Impact on Kids Content,* SSRN (2024) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4430334).
60. Campbell *et al*, "Cancer Peer Support Programs—Do They Work?" *Patient Education and Counseling* 55:1 (2004) at 3-15 (available at https://www.sciencedirect.com/science/article/pii/S073839910300301X?via%3Dihub).
61. National Oceanic and Atmospheric Administration Fisheries, "National Bycatch reduction Strategy," (available at https://www.fisheries.noaa.gov/international/bycatch/national-bycatch-reduction-strategy#what-is-bycatch)
62. National Standard 9-Bycatch, 50 CFR § 600.350 (2018).
63. Taylor Telford, "Younger women are practicing radical pay transparency on TikTok," *Washington Post* (July 6, 2024) (available at https://www.washingtonpost.com/business/2024/07/04/young-women-pay-transparency-tiktok/).
64. Deposition of Patricia Shih Blough (June 27, 2024).
65. Deposition of Jacob Leady (June 25, 2024).
66. U.K Competition & Market Authority, *Online Platforms and Digital Advertising Market Study, Appendix K,* (July 1, 2020) at ¶¶8 (available at https://assets.publishing.service.gov.uk/media/5fe49595d3bf7f089f9998ce/Appendix_K_-_consumer_controls_over_platforms__data_collection_WEB.pdf).
67. Deposition of Bernadine Griffith (June 26, 2024).
68. Security Planner, *Consumer Reports* (available at https://securityplanner.consumerreports.org/) (accessed at 7/7/2024).
69. Privacy Badger, *Electronic Frontier Foundation* (available at https://privacybadger.org/) (accessed at 7/7/2024).

70. Protection for Your Digital Age, *Norton* (available at https://buy-static.norton.com/norton/ps/bb/ushard/360/us_en_nort_brfr-ft30.html) (accessed at 7/7/2024).
71. Beales and Stivers, *An Information Economic Without Data*, SSRN (2022) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4279947).
72. Todd Feathers *et al,* ""Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies," *The Markup* (December 13, 2022) (available at https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies).
73. "Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking," *Federal Trade Commission: Office of Technology* (March 16, 2023) (available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking).